Cassandra Crossing/ Apocalisse Quantistica

(618)—E' ormai necessario prepararsi alla decrittazione prossima ventura di tutto quanto è stato crittografato fino ad oggi

---

Cassandra Crossing/ Apocalisse Quantistica

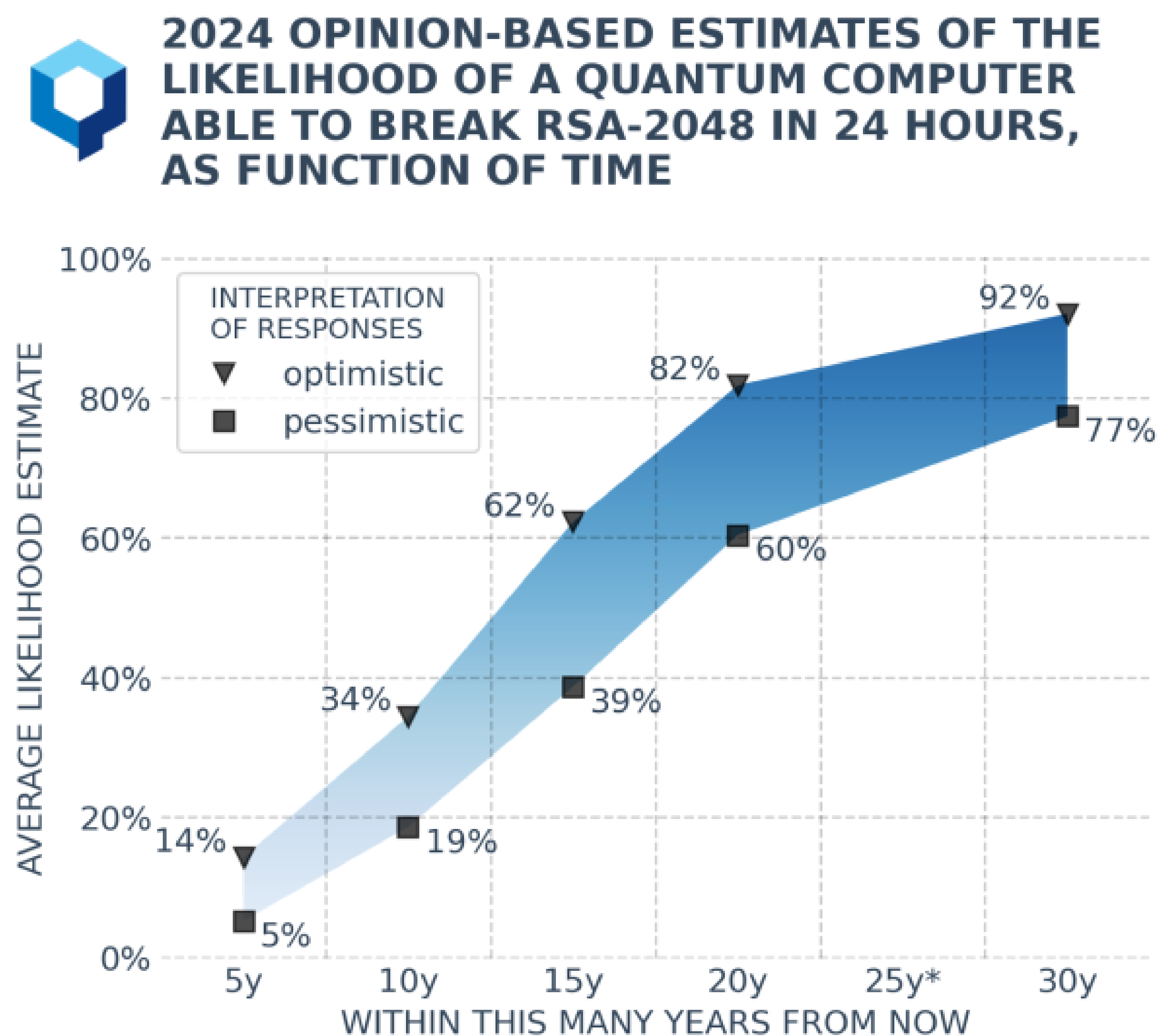


Figure 1: Global Risk Institute & RevolutionQ—Quantum threat timeline report

(618)—E' ormai necessario prepararsi alla decrittazione prossima ventura di tutto quanto è stato crittografato fino ad oggi

23 aprile 2025—I progressi, annunciati come decisivi, della realizzazione di componenti per un calcolatore quantistico sono divenuti quasi quotidiani, e poiché sono sempre stati non risolutivi, hanno prodotto assuefazione e perdita di interesse sull'argomento.

Persino Cassandra, che aveva nel cassetto una bozza per questo pezzo da un paio d'anni, era caduta preda di questo disinteresse; infatti oggi si è vista superata da Wired, che ha appena pubblicato un articolo su questo tema.

Trascurare od ignorare l’avvento dei computer quantistici è pericoloso. Vediamo perché, con un piccolo excursus storico.

La crittografia permea ormai il mondo digitale, ed impedisce attacchi, truffe ed atti di guerra, consentendo di mantenere il segreto dove serve, nonché certificare e firmare quello che serve.

Praticamente tutta la crittografia del mondo è basata su di un unico problema matematico; dato il prodotto di due numeri primi molto grandi, trovare i due fattori.

Questo problema, per numeri sufficientemente grandi, è irresolubile con i computer e gli algoritmi oggi esistenti. E’ dagli anni ’70 del secolo scorso che la riservatezza e l’autenticità delle trasmissioni di dati e dei dati stessi vengono assicurate da algoritmi basati su questa certezza; che **nessuno possa calcolare rapidamente i fattori primi.**

I crittografi di ieri hanno fatto un eccellente lavoro, ma non avevano considerato la possibilità che venissero realizzati computer con proprietà radicalmente diverse da quelli digitali oggi comuni; i computer quantistici.

Questi computer, ad oggi ancora non disponibili, sono basati sullo sfruttamento degli effetti quantistici della materia; saranno formati da “bit quantistici” o QBit, e permetteranno di risolvere molto rapidamente certe classi di problemi matematici tra cui, appunto, la fattorizzazione dei numeri primi.

Potranno fare questo facendo girare algoritmi appositi, oggi già disponibili ma che non possono essere eseguiti in maniera efficiente sui normali computer digitali, ma solo sui futuri computer quantistici.

Fine dell’excursus storico.

Perché il titolo parla di “**Apocalisse Quantistica**”?

“*Apocalisse*” (da , *apokálypsis)* è un termine greco che significa “*rivelazione*”.

Il giorno in cui i primi computer quantistici saranno operativi, eseguendo gli algoritmi quantistici già oggi disponibili, tutti i dati crittografati diventeranno potenzialmente accessibili a chi disponga di questi computer.

Proprio come raccontato nell'ultimo capitolo della Bibbia, durante questa *apocalisse digitale* “*... tutto verrà rivelato*”.

Da quella data, dal ***Q-Day***, tutte le trasmissioni crittografate, tutti i dati cifrati, diventeranno facilmente accessibili per i possessori di computer quantistici.

Ma è peggio di così; non da oggi ma addirittura da molti anni le superpotenze, certamente Cina e Stati Uniti, stanno archiviando dati e trasmissioni cifrati, per decrittarli appena disporranno di computer quantistici, in modo da carpire quelle informazioni che, pur datate, resteranno importanti.

I nostri dati riservati, i dati riservati di tutti, diventeranno liberamente disponibili alle previdenti superpotenze che li hanno archiviati.

Tuttavia, come le *vergini sagge* della “*parabola delle dieci vergini*”, ci si può preparare anche all'apocalisse, evitandone almeno una parte.

Infatti già da oggi è possibile adottare algoritmi crittografici “post-quantistici” cioè basati su problemi matematici diversi dalla fattorizzazione dei numeri primi, algoritmi che non sono attaccabili nemmeno dei computer quantistici.

Ma per ora nulla si muove sotto il sole di Internet. Nelle segrete reti militari, probabilmente gli algoritmi post-quantistici sono già impiegati, ma per gli usi civili attuali nulla è ancora cambiato.

Non è per niente banale sostituire gli algoritmi crittografici attuali con quelli post-quantistici negli infiniti protocolli ed infrastrutture digitali oggi in uso. Oltre a sostituire gli algoritmi, è anche necessario sostituire tutte le chiavi crittografiche e tutti i certificati digitali oggi esistenti, che altrimenti diventerebbero inutili perché violabili o falsificabili

Sarebbero tutti ottimi motivi per cominciare subito. Ma sostanzialmente nulla si muove.

Perché?

Cassandra non lo sa, ma non è comunque il tema di oggi.

Il Q-day non è molto lontano; uno studio del Global Risk Institute dell'anno scorso stima fino al 34% la possibilità che il Q-Day accada prima del 2035, **solo dieci anni da oggi**.

L'Apocalisse Quantistica rivelerà tutti i dati del mondo, presenti e passati; i vostri e quelli di chiunque altro.

L'Apocalisse Quantistica renderà falsificabile qualsiasi documento firmato digitalmente e qualsiasi certificato digitale.

L'Apocalisse Quantistica renderà violabili tutti i sistemi informatici protetti con la crittografia odierna; le reti informatiche potrebbero essere interrotte, i computer violati, le reti elettriche spente, i missili nucleari lanciati, non c'è limite alle disgrazie che diverrebbero praticamente possibili.

Per cui preparatevi, preparate l'olio nelle lanterne perché lo *Sposo* certamente arriverà, e potrebbe essere molto presto.

Scrivere a Cassandra—Twitter—Mastodon
Videorubrica "Quattro chiacchiere con Cassandra"
Lo Slog (Static Blog) di Cassandra
L'archivio di Cassandra: scuola, formazione e pensiero

***Licenza d'utilizzo**: i contenuti di questo articolo, sono sotto licenza Creative Commons Attribuzione—Condividi allo stesso modo 4.0 Internazionale (CC BY-SA 4.0),* tutte le informazioni di utilizzo del materiale sono disponibili a questo link*.*

By Marco A. L. Calamari on April 23, 2025.

Canonical link

Exported from Medium on August 27, 2025.